

## RESPONSE TO FINAL OFFICE ACTION

USSN: 09/920,554

Page 2

REMARKS

In the official action on page 2 thereof, the Examiner asserts that "the security level of a request (see column 8, lines 33-37 of McNabb) is "analogous to the trust level of the present claims." With all due respect to the Examiner, that is a misconception.

Security levels in McNabb are clearly defined as describing the sensitivity (e.g. classification) of the data of the object. (See McNabb column 8, lines 34-38 - cited by the Examiner).

McNabb fully realizes that trust is completely different concept than is either "sensitivity level" or "security level". Note the definition which McNabb provides for a trusted computer system at column 8, lines 41-45.

McNabb goes on to talk about trusted computers in his patent, but when he does so it seems to be in terms of definition given at column 8, lines 41-45. What is basically happening here is that McNabb assumes away the problem of a non trusted computing apparatus and just assumes that the system which he uses can be trusted. That is, it must have "sufficient hardware and software integrity measures that could be relied on to process sensitive or classified information..."

The present disclosure is concerned with employing integrity measures to ensure that a computer system can, in fact, be trusted.

Looking at it another way, the "security level" has to do with whether or not the user can be trusted. For example, security level asks the question "does the user have a sufficiently high security level on the computer to perform certain actions"? The level of trust works in the opposite direction. Can a user, whatever their security level might be, trust the computer that they are using to reliability "process sensitive or classified information without fear of denial of service, data theft, or corruption resulting from hostile activity" as mentioned in McNabb? That has nothing to do with their access privileges (their security level).

The applicant has, in the past, argued that McNabb does not disclose the claimed invention. The Examiner states otherwise, but only by asserting that the sensitivity level

public/rich/rpb temp/618934 response to final HP

NOV. 8. 2005 3:45PM

LADASPARRYLLP3239344145

NO. 5102 P. 4

## RESPONSE TO FINAL OFFICE ACTION

USSN: 09/920,554

Page 3

of requests is "analogous" to the trust level recited in the present claims (to use the Examiner's phraseology). Of course, saying one thing is analogous to another thing does not make necessarily it so and it is submitted that based on McNabb's own teaching, security and trust are completely two different concepts.

It is to be noted that the definition used for trust in McNabb is consistent with how the term trust is used in the present application. For example, whether or not a user can properly "trust," a computing platform can depend, for example, on many things, including whether or not the computer's BIOS has been compromised. The potential problems associated with a compromised BIOS and techniques for ensuring that the boot process is secure are discussed in the present application. See, for example, paragraphs [0035] through [0041] of the present application, noting that the following sentences can be found in paragraph [0041]:

"In the present embodiment, the integrity metric is acquired by the measurement function 31 by generating a digest of the BIOS instructions in the BIOS memory. Such an acquired integrity metric, if verified as described above, gives a potential user of the platform 10 a high level of confidence that the platform 10 has not been subverted at a hardware, or BIOS program, level."

The bottom line is that the applicant basically has several issues with the Examiner's rejection of claim 1. First, by using an analogy argument, the Examiner is in essence acknowledging that his rejection under 35 USC 102 is without merit. The Examiner is in essence admitting that McNabb does not teach and every element of the rejected claims unless some untenable analogy is made. The rejection under 35 USC 102 is improper and that the rejection would have at least have to be under 35 USC 103, that is, an obviousness rejection, since by the analogy argument the examiner is in essence changing that which McNabb teaches. However, since this rejection is really an obviousness rejection, the applicant has further issues with it, mainly:

- It is not seen how it would be obvious to modify McNabb so as to handle the recited levels of trust when McNabb basically assumes that this system enjoys the highest possible level of trust (that is, there is one level of trust in McNabb).

public/rich/rpb temp/618934 response to final HP

NOV. 8, 2005 3:46PM

LADASPARRYLLP3239344145

NO. 5102 P. 5

## RESPONSE TO FINAL OFFICE ACTION

USSN: 09/920,554

Page 4

- Moreover, if McNabb can somehow be modified to meet the objection noted above, then what prior art reference(s) does the Examiner rely upon to make such a rejection? The applicant is entitled to know the identity of the prior art and since the Examiner uses the word "analogous" in the rejection, the applicant is assuming that the Examiner must have some knowledge of some prior art, which is not disclosed in the official action, to justify the rejection. Anyway, the Examiner is either requested (i) to cite a prior art reference supporting his contentions or, if the Examiner is relying upon "facts within the personal knowledge" of the Examiner, (ii) to provide the affidavit specified by the rules of practice. (See 37 CFR 1.104(d)(2)).

With respect to claim 24, McNabb does not teach "service management process adapted to receive a service description which includes levels of trust assigned to process this within the service ..." As indicated above, McNabb knows nothing about levels of trust other than to assume that the computer platform in question has "sufficient hardware and software integrity measures" without reference to "levels of trust."

The rejections of the claims in this application, with all due respect to the Examiner, are not meritorious. Reconsideration is respectfully submitted.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 12-0450. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed

//  
//  
//  
//  
//  
//  
//  
//  
//

public/rich/rpb temp/618934 response to final HP

NOV. 8. 2005 3:46PM

LADASPARRYLLP3239344145

NO. 5102 P. 6

## RESPONSE TO FINAL OFFICE ACTION

USSN: 09/920,554

Page 5

and the petition fee due in connection therewith may be charged to deposit account no. 12-0450.

I hereby certify that this correspondence is being transmitted by facsimile transmission to the Commissioner for Patents at 1-571-273-8300 on November 8, 2005

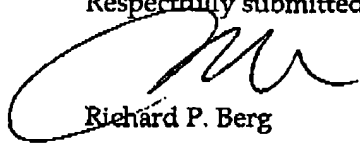
Richard P. Berg

(Name of Person Transmitting)

  
(Signature)

November 8, 2005

Respectfully submitted,

  
Richard P. Berg

Reg. No. 28,145  
5670 Wilshire Blvd., Suite 2100  
Los Angeles, CA 90036  
323-934-2300

public/rich/roh term/618994 response to final HP